Project Report

Project Title: Simulated Honeypot Deployment and Threat Monitoring Using Microsoft Azure

Project Duration: June 10–14, 2025

Objective: To simulate a vulnerable Windows environment in the cloud using Microsoft Azure, enabling real-world cyberattack monitoring and analysis using Microsoft Sentinel and Log Analytics. The goal was to understand how attackers behave and how cloud-native SIEM (Security Information and Event Management) tools like Sentinel help in detection and response.

Tools & Technologies Used

- **Microsoft Azure** (Pay-As-You-Go subscription)
- **Windows 10 Enterprise LTSC 2021 VM**
- **Azure Log Analytics Workspace**
- **Microsoft Sentinel**
- **Azure Network Security Groups (NSG)**
- **Public IP Address (Dynamic)**
- **Azure Resource Groups & Virtual Network (VNet)**

Step-by-Step Execution

1. Virtual Machine Setup:

- Created a Windows 10 Enterprise VM in the East US 2 region (Zone 1).
- Used B1ls SKU for low-cost deployment.
- Enabled RDP and opened multiple ports to mimic an insecure setup.

2. Networking Configuration:

- Created NSG with open inbound rules (RDP, SMB, HTTP, and high-risk ports).
- Associated NSG with the subnet and VM's network interface.

3. Log Analytics Workspace:

- Provisioned a workspace to collect telemetry data from the VM.
- Installed and configured the Microsoft Monitoring Agent on the VM.

4. Microsoft Sentinel Integration:

- Enabled Microsoft Sentinel on the Log Analytics Workspace.
- Activated built-in rules for suspicious RDP behavior, port scans, and failed logins.
- Used Sentinel dashboards and Workbooks to visualize and investigate activities.

5. Threat Simulation:

- Opened ports and let the VM sit exposed to the internet.
- Observed attempted brute-force logins and port scans in Sentinel.

6. Cleanup & Cost Control:

- Deleted the VM, disks, public IP, Log Analytics workspace, and Sentinel solution.
- Verified no remaining billable resources.